CLAIMS

Therefore, having thus described the invention, at least the following is claimed:

1. A system for providing network-based firewall policy configuration and facilitation, comprising:

a firewall facilitation coordinator configured to receive a request to add an application not currently supported by a user's firewall policy, and to generate a time window during which a user can run the application; and

a policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured to receive a firewall modification request from the firewall facilitation coordinator, to be aware of communications or packets observed by the firewall during the time window, and to modify the user's firewall policy.

2. The system of claim 1, further comprises a firewall process adapted to communicate with the policy modification agent, the firewall process includes the user's firewall policy, a firewall communications or packet inspector and a firewall filter.

3. The system of claim 2, wherein the firewall facilitation coordinator is further configured to decode and decrypt the firewall modification request, and further configured to authenticate the user before taking action on the request.

4. The system of claim 3, wherein the firewall facilitation coordinate further comprises at least one of a secure transceiver, a firewall facilitation coordinator controller, a user notification authenticator, a user database, or a firewall policy configuration/modification window generator.

5. The system of claim 4, wherein the policy modification agent further comprises at least one of a secure transceiver, policy modification agent controller, policy modifier, blocking history checker or blocking database.

6. The system of claim 5, wherein the user exercises the application during the time window with that application transmitting/receiving communications or packets through the network-based firewall with communications or packets associated with the application passing through the network-base firewall unblocked.

7. The system of claim 5, wherein during the time window, the policy modification agent via the firewall process examines communications or packets associated with the application and modifies the user's firewall policy such that the communications or packets are allowed to pass through the firewall process unblocked.

8. The system of claim 1, further comprises a blocking history checker for checking communications or packets observed during the time window to be associated with the application in order to identify questionable communications or packets which are defined as those communications/packets or communications/packet types that are already part of the user's firewall policy or communications or packets previously blocked at times other than during the time window but which are now observed during the time window.

9. The system of claim 8, wherein the policy modification agent is configured to not modify the user's firewall policy to include the questionable communications or packets.

10. The system of claim 9, wherein the policy modification agent is configured to record the questionable communications or packet types in a blocking history database.

11. The system of claim 10, wherein the policy modification agent is configured to send an acknowledgement of questionable communications or packet types recorded in the blocking history database to the user via the firewall facilitation coordinator.

12. The system of claim 10, wherein the policy modification agent is configured to attempt to modify the user's firewall policy a configurable number of times and if

unsuccessful, to notify the user/customer to seek assistance or to notify appropriate personnel for assistance.

13. The system of claim 8, wherein the policy modification agent is further configured to group the types of questionable packets singly and in combination of two or more.

14. The system of claim 13, wherein the policy modification agent is further configured to prioritize the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

15. The system of claim 13, wherein the policy modification agent is further configured to perform successive policy modification attempts to remove previously added questionable packet groups and to add the next highest priority group to the firewall policy.

16. A method for modifying a firewall policy of a network-based firewall, comprising:

notifying a coordinating entity of a request to modify the firewall policy to incorporate filtering rules to allow communications or packets from a new application to pass through the network-based firewall without being blocked;

notifying a policy modifier of the modification request;

sending a user an indication of a time period during which the user can exercise a new application; and

examining the communications or packets traversing to/from the network-based firewall from/to the user and modifying the user's firewall policy such that necessary communications or packets associated with the new application are allowed to pass through the network-based firewall.

17. The method of claim 16, further comprising acknowledging the modification request and sending an acknowledgement of the modification request to a user's processing device.

18. The method of claim 16, further comprising authenticating the user before acting on the modification request.

19. The method of claim 16, wherein notifying a coordinating entity and a policy modifier of a request to modify a firewall policy step further comprises providing a name of the new application and a time frame for implementation of configuration change.

20. The method of claim 16, further comprising sending an acknowledgement of completion of the modification to the user's processing device.

21. The method of claim 16, further comprising blocking communications or packets not associated with filtering rules associated with the new application.

22. The method of claim 16, further comprising inspecting received communications or packets and checking a blocking history to identify questionable communications or packet types which are defined as those communications/packet types observed during the time window to be associated with the application but which are already included in the firewall policy or communications/packet types which were previously blocked at times other than during the time window but which are now observed during the time window.

23. The method of claim 16, further comprising modifying the firewall policy rules formed for the new application to provide for blocking the questionable communications or packets.

24. The method of claim 16, further comprising recording the questionable communications or packet types in a blocking history database.

25. The method of claim 16, further comprising sending an acknowledgement to the user's processing device to repeat an attempt to modify firewall policy when the new application does not function properly through the network-based firewall.

26. The method of claim 16, further comprising notifying the user's processing device after a configurable number of repeat attempts that fail to modify the firewall policy such the new application can function properly through the firewall.

27. The method of claim 16, further comprising allowing communications or packets associated with the new application to pass through the network-based firewall.

28. The method of claim 22, wherein the examining step further comprises grouping the types of questionable packets singly and in combination of two or more.

29. The method of claim 28, wherein the examining step further comprises prioritizing the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and labeling the groups in order of priority.

30. The method of claim 28, wherein examining step further comprising performing successive policy modification attempts to remove previously added questionable packet groups and adding the next highest priority group to the firewall policy.

31. A computer-readable medium for providing network-based firewall policy configuration and facilitation, comprising:

logic configured to notify a coordinating entity of a request to modify a firewall policy to incorporate filtering rules to allow communications or packets from a new application to pass through the network-based firewall without being blocked;

logic configured to notify a policy modifier of the modification request;

logic configured to send a user an indication of a time period during which the user can exercise a new application; and

logic configured to examine the communications or packets traversing to/from the network-based firewall from/to the user and modifying the user's firewall policy

such that necessary communications or packets associated with the new application are allowed to pass through the network-based firewall.

32. The computer-readable medium of claim 31, further comprising logic configured to acknowledge the modification request and logic configured to send an acknowledgement of the modification request to a user's processing device.

33. The computer-readable medium of claim 31, further comprising logic configured to authenticate the user before acting on the modification request.

34. The computer-readable medium of claim 31, wherein the logic configured to notify a coordinating entity and a policy modifier of a request to modify a firewall policy is further includes logic configured to provide a name of the new application and a time frame for implementation of configuration change.

35. The computer-readable medium of claim 31, further comprising logic configured to send an acknowledgement of completion of the modification to firewall facilitation coordinator and to the user's processing device.

36. The computer-readable medium of claim 31, further comprising logic configured to block communications or packets not associated with filtering rules associated with the new application.

37. The computer-readable medium of claim 31, further comprising logic configured to inspect received packets and logic configured to check blocking history to identify questionable communications or packet types which are defined as those communications or packet types already included in the firewall policy or communications or packet types which were previously blocked at times other than during the time window but which are now observed during the time window .

38. The computer-readable medium of claim 31, further comprising logic configured to modify the firewall policy rules formed for the new application to provide for blocking previously blocked communications or packets.

39. The computer-readable medium of claim 31, further comprising logic configured to inspect received communications or packets and to check a blocking history to identify questionable communications or packet types which are defined as those communications/packet types observed during the time window to be associated with the application but which are already included in the firewall policy or communications/packet types which were previously blocked at times other than during the time window but which are now observed during the time window.

40. The computer-readable medium of claim 31, further comprising logic configured to modify the firewall policy rules formed for the new application to provide for blocking the questionable communications or packets.

41. The computer-readable medium of claim 31, further comprising logic configured to record the questionable communications or packet types in a blocking history database .

42. The computer-readable medium of claim 31, further comprising logic configured to send an acknowledgement to the user's processing device to repeat an attempt to modify firewall policy when the new application does not function properly through the network-based firewall.

43. The computer-readable medium of claim 31, further comprising logic configured to notify the user's processing device after a configurable number of repeat attempts that fail to modify the firewall policy such that the new application functions properly through the network-based firewall.

44. The computer-readable medium of claim 31, further comprising logic configured to allow the communications or packets associated with the new application to pass through the network-based firewall.

45. The computer-readable medium of claim 37, further comprising logic configured to group the types of questionable packets singly and in combination of two or more.

46. The computer-readable medium of claim 45, further comprising logic configured to prioritize the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

47. The computer-readable medium of claim 45, further comprising logic configured to perform successive policy modification attempts to remove previously added questionable packet groups and to add the next highest priority group to the firewall policy.